Whitelist Cisco IronPort (ESA)

Whitelist Cisco IronPort (ESA) for CyTech – AQUILA Phishing Simulation

Why Whitelist in Cisco IronPort?

Whitelisting ensures that the CyTech - AQUILA Phishing Simulation (PS) emails are delivered without interference from Cisco IronPort's anti-spam and threat detection filters. Without proper configuration, PS emails may be quarantined, flagged, or altered, impacting the accuracy and effectiveness of the training.

To ensure proper delivery, the following configurations are recommended:

- IP Allow List (HAT Policy)
- Mail Flow Policies (Mail Policy)
- Content Filters (Bypass ATP and anti-spam)
- Domain and URL Filtering

Key Configurations

1. Whitelist Sending IP Addresses (HAT Policy - Mail Flow Policy)

Steps:

1. Log in to Cisco IronPort (ESA) via the web interface.
2. Go to **Mail Policies > HAT Overview**.
3. Edit the **Incoming Mail Policy** or create a new one for CyTech Phishing Simulation.
4. Under the "Sender Group", create a new entry (e.g., **AQUILA-Phish**).
5. Add the following IPs: Mail Server and Landing Page

```
35.153.237.243
```

```
107.22.65.180
```

6. Set the **Mail Flow Policy** for this group to **ACCEPTED**.

> This ensures AQUILA emails are not rejected or throttled by IP filtering.

---

2. Whitelist Domains and Header-Based Filtering (Message Filters)

To ensure messages are recognized as simulations and not flagged, configure a custom header filter.

Steps:

1. Navigate to **Mail Policies > Message Filters**.
2. Add a new filter named **Cytech_Header_Bypass.**

Filter Syntax Example:

```
CyTech_Header_Bypass:
if (header("X-PHISHTEST") == "CYTECH") {
   skip-spamcheck();
   skip-viruscheck();
   skip-attachmentcheck();
   log-entry("CyTech Simulation Bypass");
}
```

3. Commit changes and enable the filter.

---

3. Create a Content Filter to Bypass Anti-Spam & ATP (Content Filters)

Steps:

1. Go to **Mail Policies > Content Filters**.
2. Add a new filter (e.g., **AQUILA_Bypass_SPAM_ATP**).
3. Create a condition using either:

- **Sender IP**: match any of the CyTech IPs.
  - **35.153.237.243**
  - **107.22.65.180**
- **Sender Domain**: match domains listed below.

Domains to Whitelist:

```
slackj.com
ttrelli.com
airbnd.cc
attlassians.com
eebbey.com
lastpasss.net
my1psswords.com
zooms.cc
0365.click
micros0ft.click
offlce.click
```

Actions:

- Bypass spam and virus filters.
- Optionally log a custom message.
- Tag emails if needed for internal monitoring.

4. Commit changes.

---

4. URL Filtering / Allow List (Optional - Web Reputation / AMP Integration)

If you have Cisco AMP or Web Reputation Filters enabled:

Steps:

1. Navigate to **Security Services > URL Filtering / Web Reputation Filters**.
2. Add the following simulation URLs to the **Allow List** or mark as **Trustworthy**:

```
slackj.com/*
ttrelli.com/*
airbnd.cc/*
attlassians.com/*
eebbey.com/*
```

```
lastpasss.net/*
my1psswords.com/*
zooms.cc/*
0365.click/*
micros0ft.click/*
offlce.click/*
```

5. Prioritize Rules (Recommended)

Ensure that the HAT, content filters, and message filters for CyTech Phishing Simulation have the **highest priority** or are evaluated **before** other blocking rules.

Final Checklist

- [ ] IPs whitelisted in HAT policy
- [ ] Custom header filtering configured (X-PHISHTEST: CYTECH)
- [ ] Content filters bypass spam/virus checks
- [ ] Simulation domains and URLs allowed
- [ ] Filters/rules are enabled and prioritized correctly

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #2
Created 10 June 2025 10:41:20 by Richmond Abella
Updated 11 July 2025 06:37:07 by Richmond Abella